Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for Law	)	
Enforcement Act	)	CC Docket No. 97-213
	)	

Ameritech Comments
on Notice of Proposed Rulemaking

The Ameritech Operating Companies[1] respectfully submit its comments in the Federal Communication Commission's Notice of Proposed Rulemaking issued in CC Docket No. 97-213, In the Matter of the Communications Assistance for Law Enforcement Act. In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) which imposes certain obligations on telecommunications carriers. Specifically, CALEA requires telecommunications carriers subject to the Act to expeditiously isolate, intercept and deliver wire and electronic communications to law enforcement, and to expeditiously isolate and enable law enforcement access to call identifying information that is reasonably available.

Within the Act, the FCC was given certain responsibilities to ensure the proper implementation of CALEA. The FCC then issued its Notice of Proposed Rulemaking in the above captioned matter requesting comments on specific issues. Ameritech's comments are discussed below.

[1] The Ameritech Operating Companies are Ameritech Illinois, Ameritech Indiana, Ameritech Michigan, Ameritech Ohio, and Wisconsin Bell, Inc. d/b/a Ameritech Wisconsin.

A. Comments

1. Definition of Telecommunications Carrier.

Ameritech supports the FCC's proposed rule to establish a broad definition of 'telecommunications carrier' to ensure that all necessary parties are required to fulfill the obligations of CALEA. Specifically, the FCC needs to ensure that resellers are considered telecommunications carriers. Ameritech notes that, in many cases, the reseller will be initially listed on the court order because the reseller provides the service to the customer, and the underlying telecommunications carrier will be unable to provide law enforcement with the accurate telephone number for that customer. Thus, from a network standpoint, the telecommunications carrier that owns and operates the switch will have to initiate the intercept, but will not have the authority or ability to initiate the intercept without the reseller's authorization. Consequently, it is imperative that resellers be included in the definition of telecommunications carrier.

2. Information Services

While the FCC concludes that information services provided exclusively by information service providers are excluded from CALEA's requirements, the FCC requests comments on whether information services provided by common carriers should be subject to CALEA. Information services regardless of the type of carrier providing the service are not subject to the capability requirements of CALEA. In fact, the CALEA statute specifically states that the capability requirements in the statute do not apply to information services.[2] The statute does not distinguish between information services

[2] 47 U.S.C. sec. 1002(b)(2).

provided by information service providers and common carriers, and there is no logical or theoretical basis for making such a distinction. Thus, the FCC cannot extend the reach of its rules and regulations beyond that granted by the statute. Therefore, there is no justification for arguing that the information services provided by common carriers should be subject to CALEA.

3. Definition of Appropriate Authorization under Section 229(b)(1).

The FCC proposes to define "appropriate authorization" under Section 229(b)(1) as the necessary authorization by the carrier to an employee prior to the implementation of an intercept. Ameritech disagrees with the proposed definition and believes that the "appropriate authorization" required by Section 229(b)(1) refers to the necessary authorization from law enforcement, in most cases a court order, received prior to implementing an intercept. Nothing in the congressional records or statute indicates that the statutory language was intended to dictate a corporation's *internal business process* for implementing an intercept. Most corporations, including Ameritech, grant authority to employees as part of the job function and do not require continual re-authorization for employees to perform their job duties. In this regard, Ameritech has a specific division dedicated to implementing court orders for intercepts and performing other security functions. These employees have considerable experience in performing their jobs and Ameritech relies on their expertise to ensure that the work is done properly. These employees have as their job function the responsibility to review court orders to ensure all necessary information is provided and to initiate the intercept.

The FCC's proposed definition establishes an unnecessary and bureaucratic overlay on the process of implementing intercepts. Specifically, the FCC's proposal to require

prior employee authorization before implementing an intercept would necessarily require one employee who grants the authorization to review all court orders for their credibility prior to granting the other employee the authorization to implement the intercept. There is no logical justification for this outcome.

Moreover, the FCC should clarify its definition of appropriate authorization under Section 229 of the Communications Act for the purposes of implementing Section 105 of CALEA. In this regard, the FCC proposes that a letter from a senior law enforcement official stating that a court order is unnecessary constitutes sufficient authorization. While Ameritech has complied with such requests previously and will continue to do so, unless the intercept is activated pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), Ameritech also requires that a court order be provided within a 24 to 48 hour period in order to continue the intercept. The FCC's proposed rule should be clarified to reflect this safeguard.

4. Vicarious Liability of Carrier for Unlawful Intercepts.

The FCC requests comments on carriers' vicarious liability for unlawful intercepts.[3] Ameritech agrees that it has the responsibility to prevent its employees from initiating unlawful intercepts, and Ameritech strongly enforces it policies to prohibit such activity. Unless a telecommunications carrier fails to monitor and enforce its policies against such activities, corporations will not be held liable for the unlawful acts of its employees. Thus, in most instances, corporations will not be found vicariously liable for unlawful intercepts performed by their employees in violation of the corporations' policies.

[3] NPRM at paragraph 27.

Consequently, reporting an unlawful intercept to the FCC will not mitigate or modify their liability, since corporations will not be liable in the first instance.

In addition, Ameritech objects to any requirement to report employees' misconduct to the FCC. Ameritech already reports any unlawful intercepts to law enforcement in order for law enforcement to take proper action. In fact, given the privacy considerations regarding intercepts in general-- and unlawful intercepts in particular -- this proposed reporting requirement to the FCC does not provide any additional protection, but adds additional risk of exposure of the violated party.[4]

5. Internal Carrier Security.

The FCC has a number of different proposals regarding internal carrier security. Specifically, the FCC proposes: 1) each employee involved in an intercept sign an affidavit for each and every intercept, and the affidavit contain specific information regarding the intercept; 2) carriers keep specific information about each and every intercept for 10 years; and 3) the internal carrier security measures be filed with the FCC for review.

For the most part, Ameritech supports the FCC's proposals for internal carrier security. Ameritech already maintains the records requested by the FCC regarding the

[4] In fact, Ameritech questions whether it would have the authority to actually disclose that information to the FCC. Title 18 only allows telecommunications carriers to assist persons authorized to receive the intercepted information, and CALEA provides that telecommunications carriers only provide intercepted information to the government, which is defined as federal or state agencies "authorized by law to conduct electronic surveillence." See 47 U.S.C. secs. 1001(5) and 1002. In fact, when Ameritech performs intercepts of the same party for different government agencies, Ameritech is unable to tell one agency about the intercept by a different agency. To the contrary, Rule 64.1703 in the NPRM proposes that an "employee or officer of a telecommunications carrier shall assist in intercepting and disclosing *to a third party*...." This language implies that a telecommunications carrier would have authority to disclose intercept information to a third party. It appears that this rules goes significantly beyond what is authorized by the statute, and therefore needs to be clarified consistent with the language in Title 18 and CALEA.

implementation of the intercept except for the information about the time during which the intercept is initiated and/or terminated. Ameritech would also recommend that corporations maintain copies of the legal authorization, i.e., court order or letter authorizing the intercept. In addition, Ameritech supports the FCC's proposal to file its internal carrier security policy with the FCC for review pursuant to the requirements in Section 229 of the Communications Act.

However, with regard to maintaining the records, Ameritech disagrees with the proposal to maintain these records for ten (10) years. There is no existing requirement and no logical justification for it.[5] Moreover, Ameritech does not agree with the FCC's proposal to make these record keeping obligations apply to only certain carriers based on total revenue. In this regard, there is no correlation between revenues and the number of intercepts initiated by a carrier. It appears that geographic location has more impact than revenues on the potential number of intercepts a carrier will be required to implement. In fact, the FBI acknowledged the importance of geographic location in its Second Capacity Notice when it stated that each carrier operating in a county would have to meet the capacity requirements of the county regardless of the type of equipment used or customer base.[6] Thus, telecommunications carriers operating in areas in which there is a high

---

[5] It appears that this recommendation was put in to have carriers' records act as a backup for law enforcement's requirement to maintain intercept information pursuant to 18 U.S.C. sec. 2518(8)(a). Law enforcement's requirement is related to the judicial proceedings which would use or rely on such evidence. CALEA was designed to expedite intercepts. It is not designed for the FCC or law enforcement to establish any rule beneficial to them regarding the recordkeeping of intercept information. Thus, there is nothing in the CALEA legislation which provides a justification for imposing the cost and expense of this recordkeeping requirement on telecommunications carriers.

[6] See Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, Second Notice and Request for Comments on the Actual and Maximum Capacity Requirements, 62 Fed. Reg.

concentration of intercepts should be under the same obligations to keep records and file internal carrier security policies as other telecommunications carriers. This is the only way to ensure the privacy and security interests of all individuals.

Finally, requiring employees to create and execute affidavits prior to implementing all intercepts does not serve to protect either law enforcement, the corporation or the privacy interests of the individual. Under the FCC's proposal any employee involved in the implementation of an intercept would have to sign an affidavit containing all the information relevant to that intercept.[7] Ameritech has been implementing these intercepts for years. Given the sensitive nature of the intercepts, Ameritech has limited the knowledge of all aspects of the intercepts to the least amount of people as possible. In this regard, while some individuals will understand they are doing work to implement an intercept, these individuals will not have full knowledge regarding the line, the persons, the timing, the authorization, etc. Limiting this type of information to as few people as possible protects them and the company from undue influence.

In contrast, the FCC's proposal would require that several individuals now sign affidavits giving them full knowledge about all aspects of the intercept. Ameritech believes this strongly compromises the ability to keep the information as confidential as possible. Moreover, as with the FCC's proposal to require appropriate **internal**

[7] While the FCC would exclude "non-designated" employees from filling out the affidavits, it is unclear who would be considered non-designated employees. In this regard, there are field people who implement intercepts, but those individuals initiating the network piece has no knowledge of who is being tapped, when, where or why.

authorization with each intercept, the proposal creates an unnecessary, expensive and risky internal process.

Based on the foregoing, Ameritech supports the FCC's proposal to keep records for each intercept, and to maintain and file for FCC review an internal carrier security policy. However, Ameritech believes that all carriers that operate in a certain geographic area should be subject to the same record keeping obligations and the FCC should not adopt the proposed employee affidavit requirements.

6. Extension of Compliance Date.

The FCC proposes to "permit carriers to petition the FCC for an extension of time under Section 107, on the basis of the criteria specified in Section 109."[8] Under this proposal it appears that the FCC confuses the standards under which carriers are allowed to request for extensions of time under Section 107 with extensions of time under Section 109.

Specifically, Section 107 provides that carriers may petition for an extension of time for complying with Section 103, and the FCC may grant that extension on the grounds that "compliance with the assistance capability requirements under Section 103 is not reasonably achievable *through the application of technology available within the compliance period.*"[9]

Section 107 allows for an extension recognizing that the technical capability may not exist in the timeframe necessary for compliance. One factor the FCC should consider

---

[8] See NPRM at paragraph 50.

[9] 47 U.S.C. sec. 1006(c)(emphasis added).

when determining whether to grant an extension under Section 107 is whether a technical standard is established. Specifically, the FCC should consider the complexity of the capability requirements and the amount of time and effort needed to understand the requirements and to develop them. A second factor that FCC should consider is that it will take a minimum of twenty-four months from the adoption of a technical standard to the actual implementation of that technology in the network. In its Implementation Plan filed with Congress in March, 1997, the FBI acknowledged that the 24 month timeframe between adoption of a standard and implementation of technology was a reasonable timeframe. Specifically, the FBI stated in its Implementation Plan that this 24 month timeframe is a "factor the Commission should consider in determining whether CALEA's assistance capability requirements are reasonably achievable within the compliance period."

Finally, a third factor the FCC should consider in determining whether to grant an extension of time under Section 107 is the status of the FBI's Final Notice of Capacity. The FBI has yet to issue is final notice on the actual number of intercepts telecommunications carriers must be able to perform for law enforcement. While the technology standard is currently focused on what the capability requirements are under the statute, the actual number of interceptions telecommunications carriers will have to provide to law enforcement, i.e., the capacity requirements, is an integral part of those capability requirements.

Based on the foregoing, in determining whether to grant an extension under Section 107, the FCC should consider: 1) the availability of technology necessary to comply with CALEA; 2) the complexity of the technical issues to be addressed; 3) the progress made

toward addressing those technical issues; and 4) the timing of the release of the FBI's Final Notice of Capacity requirements.

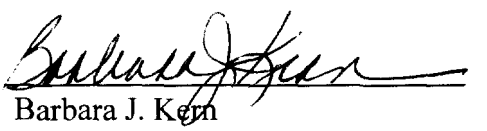
On the other hand, Section 109 provides that carriers may petition the FCC for extension of compliance with Section 103 with respect to any equipment or services installed or deployed after January 1, 1995. The FCC may grant the extension if it finds that the compliance is not "reasonably achievable" by determining "whether compliance would impose significant difficulty or expense on the carrier...."[10] In contrast to Section 107's focus on technology, Section 109 focuses on the economic costs of complying with CALEA for that equipment and services installed or deployed after January 1, 1995. Under the current statute, carriers are responsible for the costs of making this category of equipment and services comply. Thus the factors which are listed in the statute and which the FCC should use are economic factors. These sections provide two different avenues aimed a two different purposes for granting extensions.

[10] 47 U.S.C. 1008(b).

B. Conclusion.

Ameritech respectfully submits the comments and requests the FCC to adopt its proposed rules and regulations modified as requested above.

Respectfully submitted,



Barbara J. Kern
Counsel
Ameritech Corporation
2000 West Ameritech Center Drive
Room 4H74
Hoffman Estates, IL 60196
(847) 248-6077

December 12, 1997